

# 1, 2, and 6 qubits, and the Ramanujan-Nagell theorem

**Yaroslav Pavlyukh**

Institut für Physik, Martin-Luther-Universität Halle-Wittenberg, Heinrich-Damerow-Str. 4,  
06120 Halle, Germany

E-mail: [yaroslav.pavlyukh@physik.uni-halle.de](mailto:yaroslav.pavlyukh@physik.uni-halle.de)

**A. R. P. Rau**

Department of Physics and Astronomy, Louisiana State University, Baton Rouge, LA 70803,  
USA

E-mail: [arau@phys.lsu.edu](mailto:arau@phys.lsu.edu)

**Abstract.** A conjecture of Ramanujan that was later proved by Nagell is used to show on the basis of matching dimensions that only three  $n$ -qubit systems, for  $n = 1, 2, 6$ , can share an isomorphism of their symmetry groups with the rotation group of corresponding dimensions 3, 6, 91. Topological analysis, however, rules out the last possibility.

PACS numbers: 03.67.-a, 42.50.Dv, 02.40.Re, 02.20.Qs

Consideration of a single qubit in terms of rotations in three dimensions is familiar from the earliest days of nuclear magnetic resonance (nmr) and the use of such a “Bloch sphere” recognized widely as of great value both in nmr and its applications and in quantum information [1, 2, 3]. Equally, in dealing with two qubits and their algebra of 15 generators of  $SU(4)$ , the correspondence to the 15 antisymmetric matrix operators of the six-dimensional rotation group  $SO(6)$ , with products of the two sets of Pauli matrices for the two qubits rearranged in such a  $6 \times 6$  antisymmetric array has proved useful (see Eq.(B.1) of [4]). In particular, a ten-dimensional subgroup  $SO(5)$  of both plays an important role in several logic gates and in four-level systems in molecular physics and quantum optics [4]. Already current experiments [5] demonstrate the feasibility of creating multi-qubit states thus posing a question on whether such parallels can be exploited for even higher dimensional Lie groups. The aim of the present contribution is to provide both the dimensional and topological arguments that these are the only examples of accidental homeomorphisms between the qubit symmetry groups and the orthogonal groups. In the course of presentation we will refer to numerous facts from the corresponding disciplines. Therefore, our exposition will be accompanied by extensive references to mathematical texts for the interested reader.

*Dimensions of unitary and orthogonal groups* It is a curious fact that the dimension of the symmetry group of  $n$  qubits,  $SU(2^n)$ , is of the form of a Mersenne number  $2^{2n} - 1$ . Equally striking even if obvious is the connection between the mathematical/geometrical concept of triangular numbers and the number  $N(N - 1)/2$  of antisymmetric generators that define rotations in  $N$ -dimensional space, these  $SO(N)$  groups being central to physics. For the number of generators of  $SU(2^n)$  and  $SO(N)$  to coincide, we must have

$$N^2 - N = 2(2^{2n} - 1). \quad (1)$$

This quadratic equation in  $N$  has integer solutions only when the discriminant is a perfect square, that is, when

$$2^{2n+3} = k^2 + 7, \quad (2)$$

with  $k$  an integer.

One hundred years ago in 1913, the mathematical genius Ramanujan, with his gift for number patterns, conjectured that only a few Mersenne numbers (of the form  $2^b - 1$  with  $b$  a positive integer) are triangular [6]. This corresponds to the statement that the Diophantine equation  $2^b = k^2 + 7$  has only a finite number of solutions among  $b$  and  $k$  integers. This was proved in 1948 by the mathematician T. Nagell<sup>‡</sup>, that such solutions exist only for the five conjectured values,  $b = 3, 4, 5, 7, 15$  and, correspondingly,  $k = 1, 3, 5, 11, 181$  [7, 8].

Drawing on the Ramanujan-Nagell theorem, and setting  $n = (b - 3)/2$ , we can conclude that the only physically relevant values for  $n$  qubits are the ones corresponding to the last three of their numbers, namely,  $n = 1$  with  $(b = 5, k = 5)$ ,  $n = 2$  with  $(b = 7, k = 11)$ , and  $n = 6$  with  $(b = 15, k = 181)$ . Correspondingly, the values of  $N$  are  $N = (k + 1)/2 = 3, 6, 91$ . Thus, three-dimensional rotations for a single qubit, six-dimensional rotations for a pair of

<sup>‡</sup> The original proof published in [7] is hard to access, therefore readers should consult for instance [8].

qubits and 91-dimensional rotations for a set of six qubits! But, in the next section, we show that this last possible homeomorphism can also be ruled out under further analysis.

*Topological analysis* It is sufficient to consider the simplest topological invariants (see [9] on historical perspective on terms mentioned in this manuscript) the *Betti numbers*, to see that  $SU(2^6)$  and  $SO(91)$ , even though having the same dimension, differ topologically. We will also operate with the *Poincaré polynomial* defined for a  $z$ -dimensional manifold  $M$  as

$$P(M, t) = \sum_{q=0}^z b_q(M) t^q,$$

where  $b_q$  are the Betti numbers, i.e. the *ranks* (i.e. the number of elements of its generating set) of the homology groups  $H_q(M, \mathbb{Z})$  of the manifold (very transparent introduction of homology groups can be found at [10]). By the theorem of C. Chevalley (see for example [11], p. 86) the Poincaré polynomial of a simply connected compact simple real Lie group is

$$P(t) = \prod_i (t^{2\alpha_i+1} + 1),$$

where  $\alpha_i$  are the exponents of the simple Lie group. The special unitary groups  $SU(n+1)$  belong to the class  $A_n$  (in E. Cartan classification [12]) with the exponents  $\alpha_i = 1, 2, \dots, n$  while the orthogonal group  $SO(2n+1)$  belongs to the  $B_n$  class with the exponents  $\alpha_i = 1, 3, \dots, 2n-1$ . The Poincaré polynomials given by:

$$\begin{aligned} P(SU(64), t) &= (1+t^3)(1+t^5) \cdots (1+t^{127}), \\ P(SO(91), t) &= (1+t^3)(1+t^7) \cdots (1+t^{179}) \end{aligned}$$

are, thus, different. This demonstrates the topological inequivalence of the two groups. The theorem of Chevalley applies to Betti numbers defined as ranks of homology groups with coefficients in  $\mathbb{Z}$ . Especially for  $SO(n)$  they are difficult to compute. Going to  $\mathbb{Z}_2$  presents a simplification and can also be used for establishing the inequivalence of the two groups. Detailed computation of  $H_*(SO(n), \mathbb{Z})$  and  $H_*(SO(n), \mathbb{Z}_2)$  can be found in [13] (see Sec. 3.D).

Since the exponents are of algebraic nature, this consideration of Betti numbers is also an algebraic argument. From the above argument, one can also easily see that  $SU(2) \cong SO(3)$  is the only example of homeomorphism between the  $A_n$  and  $B_n$  classes, the corresponding Poincaré polynomial being  $(1+t^3)$ . Similarly,  $SU(4) \cong SO(6)$  groups represent the single homeomorphism between the  $A_n$  and  $D_n$  classes, and the Poincaré polynomial is  $(1+t^3)(1+t^5)(1+t^7)$ .

Summarizing, we have presented a number-theoretic argument which limits the number of possible homeomorphisms between the  $n$ -qubit symmetry groups and the special orthogonal groups. Furthermore, we showed that  $SU(2) \cong SO(3)$  and  $SU(4) \cong SO(6)$  are the only homeomorphisms of this kind. Since our reasoning rests on facts from algebra and topology, we would like to demonstrate it in a more physically transparent way.

*Geometric explanation* It is desirable to have a simple explanation of the aforementioned fact assuming just basic knowledge of algebraic topology: we compare the homotopy groups<sup>†</sup> of the two spaces. The basis for this comparison is the Bott periodicity theorem [14] which applies to *stable* homotopy groups of Lie groups. For  $SO(n)$  and  $SU(n)$  the homotopy groups are independent of  $n$  if  $n$  is sufficiently large. This can be seen by constructing a *fibration* arising from the Lie group action:

$$SU(n-1) \rightarrow SU(n) \rightarrow S^{2n-1},$$

where the base is the coset space  $S^{2n-1} \cong SU(n)/SU(n-1)$  [10].

To see this, we recall that  $SU(n)$  acts transitively<sup>‡</sup> on the space  $\mathbb{C}^n$  preserving the norm  $|z_1|^2 + \dots + |z_n|^2 = 1$ . Physically this means that the propagator preserves the wave-function normalization and each quantum state  $\psi_p$  can be labeled by a point on the sphere  $p \in S^{2n-1}$ . The stabilizer of this point, i.e. all the transformations leaving the point unchanged,

$$\hat{U}_p \psi_p = \psi_p,$$

is isomorphic to  $SU(n-1)$ . This is obvious because  $\hat{U}_p$  performs a transformation on  $\mathbb{C}^{n-1} \subset \mathbb{C}^n$ , the subspace orthogonal to  $p$ . We can use now the exact homotopy sequence to compute homotopy groups of a *principal bundle*  $E(F, M)$ , where  $F$  is the fiber and  $M$  is the base manifold of the fibration (p. 76 of [15]):

$$\dots \rightarrow \pi_k(F) \rightarrow \pi_k(E) \rightarrow \pi_k(M) \rightarrow \pi_{k-1}(F) \dots$$

Since we know that  $\pi_k(S^n) = 0$  for  $k < n$  we have

$$0 \rightarrow \pi_k(SU(n)) \rightarrow \pi_k(SU(n+1)) \rightarrow 0, \quad \text{for } k < 2n$$

and analogically for the

$$SO(n-1) \rightarrow SO(n) \rightarrow S^{n-1},$$

fibration:

$$0 \rightarrow \pi_k(SO(n)) \rightarrow \pi_k(SO(n+1)) \rightarrow 0, \quad \text{for } k < n-1.$$

Thus, for  $k \leq 2n-1$  for  $SU(n)$  and for  $k \leq n-2$  for  $SO(n)$  we are in stable homotopy range, i.e. the homotopy groups are independent of  $n$ :  $\pi_k(SU(n)) = \pi_k(SU)$  and  $\pi_k(SO(n)) = \pi_k(SO)$ . This means that up to  $k = 90$  all homotopies for the two groups of interest are determined by the Bott periodicity:

$$\begin{aligned} \pi_k(U) &= \pi_{k+2}(U), \\ \pi_k(O) &= \pi_{k+4}(Sp), \\ \pi_k(Sp) &= \pi_{k+4}(O), \end{aligned}$$

<sup>†</sup> The  $k$ -th homotopy group  $\pi_k(M)$  of the manifold  $M$  is the group of continuous mappings of a  $k$ -sphere  $S^k$  into  $M$ . For  $f, g \in \pi_k(M)$  one defines the group operation  $h = f + g$  as a continuous map from a  $S^k$  into the *wedge sum* [13] of two spheres, i.e.  $S^k \rightarrow S^k \vee S^k$  followed by the  $f, g$  map from each of the two spheres into  $M$ , respectively.

<sup>‡</sup> The action of a group  $G$  on the space  $M$  is called transitive if the orbit of any element  $x \in M$  is the whole space.

where  $U$ ,  $O$  and  $Sp$  are the unitary, orthogonal and symplectic groups, respectively. Already from different periodicities one can conclude that the considered spaces are topologically distinct. Making use of well known results

$$\begin{aligned} 0, \mathbb{Z} & \quad \text{for } \pi_i(U), \quad i = 0, 1, \\ 0, 0, 0, \mathbb{Z}, \mathbb{Z}_2, \mathbb{Z}_2, 0, \mathbb{Z} & \quad \text{for } \pi_i(Sp), \quad i = 0, \dots, 7, \\ \mathbb{Z}_2, \mathbb{Z}_2, 0, \mathbb{Z}, 0, 0, 0, \mathbb{Z} & \quad \text{for } \pi_i(O), \quad i = 0, \dots, 7. \end{aligned}$$

and the fact that  $\pi_k(U) = \pi_k(SU)$  for  $k \geq 2$  and  $\pi_k(O) = \pi_k(SO)$  we observe that  $\pi_5$  groups are distinct:

$$\begin{aligned} \pi_5(SU(64)) &= \pi_5(SU) = \pi_1(SU) = \mathbb{Z}, \\ \pi_5(SO(91)) &= \pi_5(SO) = \pi_1(Sp) = 0. \end{aligned}$$

It should be noted that there is no contradiction for  $SO(3)$  and  $SO(6)$  groups: they fall outside the stable homotopy range for the  $\pi_5$  homotopy group. Finally we remark that the Bott periodicity, although formulated in pure topological terms, follows from the underlying algebraic structure of the Lie groups.

*Conclusions* We have demonstrated on the basis of the Ramanujan-Nagell theorem that  $SU(2) \cong SO(3)$  and  $SU(4) \cong SO(6)$  are the only accidental homeomorphisms between the symmetry groups of qubits and the orthogonal groups. Interestingly, another pair,  $SU(2^6)$  and  $SO(91)$  groups, also coincide in dimension but they are topologically and algebraically distinct. Even though the homeomorphism is not present, the 6-qubit system can efficiently be treated for the purpose of quantum computation by the Cartan decomposition [16].

Finally, we note a possible further relevance of our observation stemming from the fact that subgroups of the full  $SU(2^n)$  are often important in physical applications of  $n$  qubits as in our example [4] of  $SO(5)$  for  $n = 2$ . Relaxing the Ramanujan focus on Mersenne numbers, were we to consider a more general  $SU(d)$  with  $d$  an integer smaller than  $2^n$ , the condition in Eq. (2) becomes  $8d^2 = k^2 + 7$  which has many more solutions:

$$\begin{aligned} n_{i+1} &= 3n_i + k_i, \\ k_{i+1} &= 8n_i + 3k_i, \end{aligned}$$

with initial values  $(n_0, k_0) = (1, \pm 1)$ . One example is  $d = 11, k = 31, N = 16$ . Furthermore, in a  $n$ -qubit system, even though the full symmetry group  $SU(2^n)$  may not be isomorphic to a rotation group, there is a number of rotational subgroups:

$$SU(2^n) \supset SO(2^n) \supset SO(2^{n-1}) \dots$$

Such correspondences may be exploited for other systems of multiple qubits.

## Acknowledgments

One of us (ARPR) thanks the Alexander von Humboldt Stiftung for support and Drs. Gernot Alber and Jamal Berakdar for their hospitality during the course of this work.

## References

- [1] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 1998.
- [2] J. J. Sakurai. *Modern Quantum Mechanics*. Addison-Wesley Pub. Co., Reading, MA, 1994.
- [3] R. R. Ernst, G. Bodenhausen, and O. Wokaun. *Principles of Nuclear Magnetic Resonance in One and Two Dimensions*. Clarendon, Oxford, 1987.
- [4] D. Uskov and A. R. P. Rau. Geometric phases and bloch-sphere constructions for  $SU(n)$  groups with a complete description of the  $su(4)$  group. *Phys. Rev. A*, 78:022331, 2008.
- [5] Thomas Monz, Philipp Schindler, Julio T. Barreiro, Michael Chwalla, Daniel Nigg, William A. Coish, Maximilian Harlander, Wolfgang Hänsel, Markus Hennrich, and Rainer Blatt. 14-qubit entanglement: Creation and coherence. *Phys. Rev. Lett.*, 106:130506, 2011.
- [6] S. Ramanujan. *J. Indian Math. Soc.*, 5:130, 1913.
- [7] T. Nagell. *Norsk. Mat. Tidsskr.*, 40:62, 1948.
- [8] R. A. Mollin. *Advanced number theory with applications*. CRC Press, Boca Raton, 2010.
- [9] J. Dieudonné. *A History of Algebraic and Differential Topology 1900-1960*. Birkhäuser, Boston, 2009.
- [10] A. S. Schwarz and S. Levy. *Topology for Physicists*. Grundlehren der mathematischen Wissenschaften. Springer, Berlin, 2010.
- [11] B. Rosenfeld. *Geometry of Lie Groups*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 1997.
- [12] J. Fuchs and J. Schweigert. *Symmetries, Lie algebras and representations: a graduate course for physicists*. Cambridge University Press, Cambridge, 1997.
- [13] A. Hatcher. *Algebraic topology*. Cambridge University Press, Cambridge, 2002.
- [14] R. Bott. *Adv. Math.*, 4:353–411, 1970.
- [15] J. A. de Azcárraga and J.M. Izquierdo. *Lie groups, Lie algebras, cohomology and some applications in physics*. Cambridge University Press, New York, 2000.
- [16] N. Khaneja and S. J. Glaser. *Chem. Phys.*, 267:11–23, 2001.